

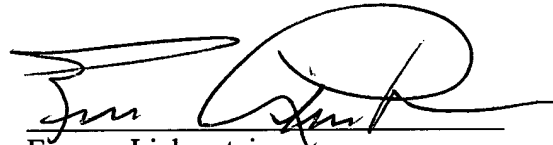
DE1484

REMARKS

This Supplemental Preliminary Amendment is being filed in order to substitute a newly amended section of page 2 for the section of page 2 previously submitted with the Preliminary Amendment filed on August 11, 2003. This is necessary because of a typographical error in paragraph (b) of that page wherein the symbol \in was typed in the place of the symbol ϵ .

It is respectfully requested that the application should now proceed to prosecution.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Eugene Lieberstein', is written over a horizontal line.

Eugene Lieberstein
Associate Attorney for Applicants
Registration No. 24,645

Dated: September 9, 2003

Anderson, Kill & Olick, P.C.
1251 Avenue of the Americas
New York, New York 10020-1182
(212) 278-1000

DE1484



APPLICANT: Myungsun KIM, et.al.

SERIAL NO. : 10/600,560

FILED : June 19, 2003

FOR : METHOD FOR IDENTIFICATION BASED ON BILINEAR DIFFIE-HELLMAN PROBLEM

EXAMINER : to be assigned

GROUP: to be assigned

CERTIFICATE OF MAILING

I hereby certify that a *SUPPLEMENTAL PRELIMINARY AMENDMENT* is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Mail Stop: Initial Patent Examination Division, US Patent & Trademark Office, POB 1450, Alexandria, VA 22313-1450 on September 11, 2003.



Audrey De Souza

Newly Amended Section of Page 2 Corresponding to the Last Paragraph

The procedure of the Fiat-Shamir scheme can be expounded as follows. A reliable system administrator selects a sufficiently large number n . Then, A prover selects his own private key a that is relatively prime with n , and calculates $b = a^2 \bmod n$. The prover discloses b . Then, the following protocol is repeated for a number of times:

(a) The prover selects a random integer $r \in Z_n^*$, where Z_n^* is a multiplicative group of order n , calculates $x = r^2$, and sends x to the verifier;

(b) The verifier selects a random number $\epsilon \in \{0, 1\}$, and sends ϵ to the prover;

(c) On receiving ϵ , the prover calculates $y = r \cdot a^\epsilon \bmod n$ and sends y to the verifier; and

(d) The verifier examines whether $y^2 = x \cdot b^\epsilon \bmod n$ is established. If true, then the verifier accepts the prover as a legitimate user and, otherwise, stops the protocol.